Claims

1. (currently amended) A hardware multiplication module, comprising:

a first input and a second input configured to receive a first operand and a second operand, respectively, represented as elements of a finite field;

an output configured to deliver a Montgomery product of the first operand and the second operand; and

a field-type ~~representation-select~~ input configured to select multiplication of the first and second operands based on ~~a selected finite field representation~~ a prime field or a binary extension field.

2. (canceled)

3. (currently amended) The module of ~~claim 2~~ claim 1, wherein the first operand is processed bit-wise and the second operand is processed word-wise.

4. (currently amended) The module of ~~claim 2~~ claim 1, wherein the second operand is divided into multiple words that are multiplied with bits of the first operand.

5. (currently amended) The module of claim 1, further comprising a dual-field adder that is configurable to execute addition without carry, based on a value supplied to the field-type select input.

6. (previously presented) A cryptographic processor, comprising:

inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field; and

a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including at least two processing units configured to determine a Montgomery product of the cryptographic parameters, each processing unit receiving a bit corresponding to the first parameter and partial words of the second parameter.

7. (original) The processor of claim 6, wherein at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit.

8. (currently amended) The processor of claim 6, further comprising a field-type~~representation-select~~ input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with $GF(p)$ or $GF(2^m)$ arithmetic, wherein $GF(p)$ is a prime field, $GF(2^m)$ is a binary extension field, p is a positive prime number, and m is a positive integer.

9. (currently amended) The processor of claim 8, wherein the arithmetic operation selectable with the field-type ~~representation-select~~ input is field addition.

10. (currently amended) The processor of claim 8, further comprising a dual-field adder in communication with the field-type~~representation-select~~ input.

11. (currently amended) The processor of claim 10, wherein the first and second cryptographic parameters are represented as m bits and e words of word length w, wherein $e = \lceil (m+1)/w \rceil$, and m, e, and w are positive integers.

12. (currently amended) A dual-field adder, comprising:

a first input and a second input situated to receive respective operands;

a field-type~~representation-select~~ input; and

an addition module, configured to add values supplied to the first and second input according to a value supplied to the field-type~~representation-select~~ input.

13. (currently amended) The dual-field adder of claim 12, wherein the field-type~~representation-select~~ input permits selection of bit-wise addition with carry or bit-wise addition without carry.

14. (original) The dual field adder of claim 13, wherein the addition module includes an exclusive OR gate situated and configured to receive a bit of the first operand and a bit of the second operand.

15. (original) The dual field adder of claim 13, wherein the addition module includes a first and a second exclusive OR gates situated and configured to receive a bit of the first operand and a bit of the second operand, respectively.

16. (previously presented) A method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising:

representing the first cryptographic parameter as a series of bits;

representing the second cryptographic parameter as a series of words;

determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage;

determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage; and

combining the intermediate values to form the Montgomery product of the first cryptographic parameter and the second cryptographic parameter.

17. (currently amended) The method of claim 16, further comprising determining intermediate values based on a field-type ~~select~~ input that selects an addition operation corresponding to addition with carry or without carry.

18. (original) A computer-readable medium containing instructions for executing the method of claim 17.

19. (currently amended) A Montgomery multiplier configured to determine a Montgomery product of a first operand and a second operand, the multiplier comprising:

a field-type ~~select~~ input for selection of arithmetic operations corresponding to a prime field or a binary extension field; and

an output that delivers the Montgomery product.

20. (currently amended) The Montgomery multiplier of claim 19, further comprising a dual-field adder that executes addition with carry or without carry based on an input delivered to the field-type ~~select~~ input.

21. (original) The Montgomery multiplier of claim 20, further comprising a scalable Montgomery multiplication module situated and configured to obtain a Montgomery product of the first operand and the second operand.